AS-СХЕМЫ ПОСТРОЕНИЯ ТАКТОВЫХ ПОДСТАНОВОК

Агиевич С. В., Марчук В. В.

БГУ, НИИ прикладных проблем математики и информатики,
факультет прикладной математики и информатики, Минск, Беларусь,
e-mail: agievich@bsu.by, siegrain7@gmail.com

Преобразования зашифрования блочно-итерационных криптосистем являются многократными композициями достаточно простых тактовых подстановок (подробнее см. [1]). Эти подстановки часто строятся по следующей схеме. Подлежащий тактовому преобразованию блок двоичных данных разбивается на фрагменты $X_1, X_2,\dots, X_n \in \{0, 1\}^m$, которые интерпретируются как векторы над полем из двух элементов. Преобразование состоит в выполнении команд двух типов: сложение пары фрагментов, замена фрагмента на S-блоке – ключезависимой подстановке S над $\{0, 1\}^m$. Операндами команд могут быть как первоначальные фрагменты, так и результаты выполнения предыдущих команд. S-блоки команд считаются произвольными, не связанными друг с другом. Результат тактового преобразования составляется из определенных фрагментов $Y_1, Y_2,\dots, Y_n \in \{0, 1\}^m$ в цепочке вычислений.

Описанной схеме вычислений мы присвоили аббревиатуру AS (от англ. addition-substitution). Сложность схемы характеризуется числом сложений и числом замен на S-блоках. Обозначения уточняются: AS_k – схемы с k заменами, $\mathrm{A}_l\mathrm{S}_k$ – схемы с k заменами и l сложениями. Число фрагментов n назовем размерностью схемы.

К классу AS_1 относятся схемы тактовых подстановок криптосистем Skipjack и SMS4. Все эти схемы имеют размерность 4.

Схемы из класса AS_1 описываются двоичным вектором $a = (a_1, a_2,\dots, a_n)$ и двоичной матрицей $B = (b_{ij})$ размера $n \times (n + 1)$:

$$Y_i = b_{i1} X_1 + b_{i2} X_2 + \dots + b_{in} X_n + b_{i,n+1} S(a_1 X_1 + a_2 X_2 +\dots + a_n X_n).$$

В докладе рассматриваются правила выбора параметров a и B. При составлении правил учитывались следующие требования по корректности, эффективности и криптографической надежности схемы: тактовые подстановки должны быть биективными; число сложений фрагментов должно быть минимальным; результат замены на S-блоке должен влиять на прообраз S-блока уже на следующем такте; линейные, разностные и линейно-разностные соотношения между фрагментами должны исчезать после минимального числа тактов; число активных S-блоков должно быть максимально большим (активный S-блок – понятие из разностного криптоанализа, см., например, [2]).

Были проведены расчеты характеристик схем из класса AS_1 размерности 4. Найдены 72 схемы, удовлетворяющие заявленным требованиям. Для всех этих схем число сложений равняется одному. Схемы Skipjack-A и Skipjack-B^{-1} попадают в число оптимальных, а схема SMS4 – нет (она не удовлетворяет только критерию минимальности числа сложений).

Литература

1. Криптология / Ю.С. Харин [и др.]. – Мн.: БГУ, 2013. – 512 с.